WEST Search History

DATE: Tuesday, May 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L7	(device near8 (managing or management)) same trap near8 (monitor or monitoring)	19	L7
L6	l2 NOT l3	27	L6
L5	((check or checking) near8 (SNMP near8 packet))	2	L5
L4	(device near8 (managing or management)) same ((check or checking) near8 (SNMP near8 packet))	0	L4
L3	L2 and SNMP	10	L3
L2	L1 and (cold adj5 start)	37	L2
L1	trap near8 (monitor or monitoring)	1387	L1

END OF SEARCH HISTORY

WEST

Generate Collection

L3: Entry 4 of 10 File: USPT Dec 11, 2001

DOCUMENT-IDENTIFIER: US 6330600 B1
TITLE: System for synchronizing configuration information of a network element if received trap sequence number is out-of-sequence

Brief Summary Text (9):
Technical advantages of the present invention include a system and method that update a memory storing configuration information of a network element using one or more state variables retrieved from the network element. In a particular embodiment, a network management server maintains configuration information for a managed network element locally and provides access to the configuration information by one or more clients in a client/server environment. The server, clients, and managed network elements communicate messages (e.g., SNMP messages) over a management network, such as an Ethernet, an Asynchronous Transfer Mode (ATM) network, or any suitable communication network. To improve access to configuration information, the server maintains one or more caches of selected configuration information readily available to clients, as well as a persistent storage of full configuration information in a database.

Detailed Description Text (4):
Each network element 16 couples to management network 20 using management links 22. Management network 20 may be a local area network (LAN), a wide area network (WAN), a public or private network, a global data network such as the Internet, a wireline or wireless network, or any other suitable communication network that provides communication among components in system 10. In a particular embodiment, management network 20 comprises an Ethernet that communicates network messages using, for example, Simple Network Management Protocol (SNMP), Remote Monitor Protocol (RMON), Transport Control Protocol/Internet Protocol (TCP/IP), or any other suitable messaging protocol.

Detailed Description Text (11):
Whether based on missed or out-of-sequence traps, local or remote modification to MIB 24, or complete or partial failure of components in system 10, there are a variety of scenarios in which server 14 must reconcile information maintained in its memory (e.g., cache 30 and database 32) to ensure a proper view and status of network elements 16. Traditionally, if there is a loss of consistency between MIB 24 and information stored in cache 30 and database 32, then server 14 initiates a full database reconciliation or synchronization to download all relevant configuration information stored in MIB 24 from network element 16. However, this operation may be slow and cumbersome, especially with significant traffic demands on a bandwidth-limited management network 20. This problem is further exacerbated by relatively crude messaging protocols (e.g., SNMP) that provide limited data integrity and lost message recovery mechanisms. Therefore, in one important aspect of the present invention, server 14 recovers from missed or out-of-sequence traps, as well as other configuration changes, without requiring a full reconciliation of cache 30 and database 32.

Detailed Description Text (17):
In operation, alarm formatter 52 monitors traps generated by network element 16 and processes the traps with special attention to missing or out-of-sequence traps. When appropriate, network monitor 56 polls for configuration information stored in MIB 24 at network element 16, and communicates set requests or other commands to modify MIB 24. Set requests may be generated locally by server 14 or by client 12 to change configuration information maintained in network element 16. While receiving autonomously generated configuration information using alarm formatter 52 or through the generation and setting of configuration information using network monitors 56, server 14 invokes configuration and alarm synchronization processes to ensure cache 30 and database 32 are consistent and synchronized with configuration information stored in MIB 24. FIGS. 3 though 7 discuss these processes in more detail.

Detailed Description Text (18):

FIGS. 3 and 4 illustrate a flowchart of a method 100 performed by network monitor 56 for synchronizing the memory of server 14 (e.g., cache 30 and database 32) with MIB 24 of a particular network element 16. Method 100 may be invoked periodically (e.g., once a day, once a week), by an operator of client 12, or autonomously by network monitor 56 or alarm formatter 52. Method 100 begins at step 102 where network monitor 56 retrieves selected state variables stored in MIB 24 and represented by a subscript "E". In a particular embodiment, network monitor 56 retrieves a set request number (SRN.sub.E), a trap sequence number (TSN.sub.E), and system up-time (SUT.sub.E) stored in MIB 24. The variable SRN.sub.E represents the number of set requests or requests to modify information stored in MIB 24. The variable TSN.sub.E represents the trap sequence number of the last trap communicated by network element 16. The variable SUT.sub.E indicates the amount of time that network element 16 has been operational since its last downtime, reboot, or other resetting event.

Detailed Description Text (20):
Network monitor 56 determines whether TSN.sub.E is less than the trap sequence number stored in NC 60 (TSN.sub.NC) at step 103, which would indicate a trap sequence reset or, more generally, a downtime, system reset, malfunction, or other failure at network element 16. If TSN.sub.E is less than TSN.sub.NC, network monitor 56 sets a trap sequence update flag (TSU) to true at step 105. Network monitor 56 then compares SRN.sub.E to the set request number maintained in NC 60 (SRN.sub.NC) at step 104. If these variables are not equal, then server 14 performs a full database reconciliation at steps 106 and 108. Network monitor 56 retrieves configuration information from MIB 24 at: step 106 and reconciles database 32 at step 108. If SRN.sub.E equals SRN.sub.NC, SRN.sub.E equals zero, and SUT.sub.E is less than the system up-time stored in NC 60 (SUT.sub.NC), then server 14 again performs steps 106 and 108 to invoke a full database reconciliation. In a particular embodiment, step 108 to reconcile database 32 is performed as follows. Server 14 initially marks each configuration entry in database 32 for network element 16 as unclean, and traverses the variables configuration tables in MIB 24 to determine whether the configuration matches. If the configuration matches, the entry in database 32 is marked as clean. If the configuration differs, the value retrieved from MIB 24 is used to update the entry in database 32, which is then marked clean-updated. If there is no entry in MIB 24, the entry is left as unclean. When the process is complete, all unclean entries are deleted.

Detailed Description Text (32):
FIG. 7 illustrates a flowchart of a method 300 performed by alarm formatter 52 to synchronize alarms at server 14. Method 300 may be invoked periodically, by a user of client 12, upon detection of a trap sequence mismatch, or by network monitor 56. Method 300 begins at step 302 where alarm formatter 52 determines whether the alarm synchronization request is from network monitor 56. If the alarm synchronization request is not from network monitor 56, then server 14 may optionally set a forced alarm synchronization flag (FAS) at step 304. By setting FAS to true, method 300 guarantees to either perform an alarm synchronization or a configuration synchronization. In contrast if FAS is false and TSN.sub.E equals TSN.sub.AC, no action to synchronize alarms will be taken.

Detailed Description Text (33):
If the alarm synchronization request is from network monitor 56 at step 302, then alarm formatter 52 retrieves the trap sequence number stored in database 32 (TSN.sub.D) at step 303. Alarm formatter 52 then determines if TSN.sub.D is greater than TSN.sub.AC at step 306 and, if true, sets TSN.sub.AC to TSN.sub.D at step 308.

Detailed Description Text (37):
FIGS. 8A and 8B illustrate processes performed by alarm formatter 52 and network monitor 56 for a variety of different trap sequence scenarios. Each scenario illustrates a timeline of receiving traps, setting and removing missing trap timer 53, and invoking configuration synchronization (CS) in accordance with method 100 and alarm synchronization (AS) in accordance with method 300. Trap sequence numbers below each timeline indicate the current state of AC 58 and NC 60 maintained by alarm formatter 52 and network monitor 56, respectively. Database 32 provides a communication mechanism for resolving any inconsistencies between information stored in AC 58 and NC 60.

Detailed Description Text (38):
Referring to FIG. 8A, scenario 400 occurs when alarm formatter 52 misses a trap. Alarm formatter 52 successfully receives traps #5 and #6, but fails to receive trap #7 as indicated by the dashed line. Upon receiving trap #8, alarm formatter 52 detects an out-of-sequence condition and sets missing trap timer 53. Upon expiration of timer 53, alarm formatter 52 invokes a configuration synchronization by network monitor 56, which

in turn invokes an alarm synchronization that reconciles the trap count in both AC 58 and NC 60.

Detailed Description Text (43):
Scenario 450 occurs when network element 16 experiences downtime, failure, or other reset event, but the cold start trap generated by network element 16 upon reset is not received by server 14. This scenario receives traps #5 and #6 successfully before the occurrence of an equipment reset. After reset, trap #1 arrives at alarm formatter 52. Since TSN.sub.E is less than TSN.sub.AC and TSN.sub.E is not in the missing trap list, alarm formatter 52 invokes a configuration synchronization. Since TSN.sub.E is less than TSN.sub.D, network monitor 56 sets TSU to true (step 105) and then performs a database reconciliation. Network monitor 56 then finishes the configuration synchronization, and since TSU is true (step 153) network monitor 56 sets TSN.sub.NC and TSN.sub.D equal to TSN.sub.E. Network monitor 56 then invokes an alarm synchronization.

WEST

Generate Collection

L7: Entry 4 of 19 File: PGPB Nov 28, 2002

DOCUMENT-IDENTIFIER: US 20020178243 A1
TITLE: Apparatus and method for centrally managing network devices

Detail Description Paragraph (24):
[0043] The integration package 140 may also comprise an initialize/resynchronize component 210, a monitor component 220, and an event notify component 230. These components may be functionally linked to the network management application 150 and are used in conjunction with the standard interface 130 to centrally manage the devices 110, 115. The initialize/resynchronize component 210 receives discovery data 202 (e.g., IP address, device ID, etc.) from the network management application 150 with respect to the devices 110, 115 on the network 120. This information may be displayed for the user via the user interface 270 and/or used by the other components to manage the devices 110, 115. For example, the monitor component 220 uses the discovery data 202 to monitor the devices 110, 115 on the network 120, and to determine device attributes as illustrated below with respect to FIG. 5 through FIG. 8. The monitor component 220 listens for messages or device traps (e.g., device failure, device error, etc.) from the devices 110, 115 on the network 120 via the standard interface 130. The event notify component 230 then notifies the administrator 280 of the status of the devices 110, 115 on the network 120.

WEST

Generate Collection

L7: Entry 6 of 19 File: USPT Oct 22, 2002

DOCUMENT-IDENTIFIER: US 6470385 B1
TITLE: Network monitoring system, monitored controller, and monitoring controller

Brief Summary Text (6):
Take an Asynchronous Transmission Mode (ATM) network for instance. In conventional monitoring systems, a point-to-point connection is established between a monitoring station and each ATM network device to be monitored, so that status information messages will be collected through the established connection. The monitoring station communicates with ATM network devices by using the Simple Network Management Protocol (SNMP), which is originally designed for TCP/IP network management. The SNMP protocol defines some techniques called "polling" and "trap" for handling of status information. Conventional network monitoring systems use this polling, trap, or both.

WEST

Generate Collection

L7: Entry 8 of 19 File: USPT Oct 27, 1998

DOCUMENT-IDENTIFIER: US 5828830 A
TITLE: Method and system for priortizing and filtering traps from network devices

Detailed Description Text (4):
The network 10 also includes a network manager 40 that is connected to the first subnet S1. Simple Network Management Protocol (SNMP) is used by the network manager 40 for managing the devices 12-38 that support SNMP. The devices 12-38 that do not support SNMP can be managed by a protocol such as Internet Control Message Protocol (ICMP). Each SNMP-manageable device stores a Management Information Base (MIB) in its memory. The MIB is a collection of objects or variables representing different aspects of the device (e.g., configuration, statistics, status, control). Each SNMP-manageable device is associated with an agent, which is a software procedure that may or may not be resident in the device. The agents monitor their associated MIBs and send out traps whenever certain conditions occur. The agents also allow the network manager 40 to access the MIB of each SNMP-manageable device. Through an agent, the network manager 40 can read values of variables from a MIB, and it can change values of variables in the MIB. Such accessibility allows the network manager 40 to perform its management tasks. For a general description of network management and SNMP, see W. Stallings, SNMP, SNMPv2 and RMON, 2d ed., Addison-Wesley Publishing Co., (1996), which is incorporated herein by reference.

WEST

Generate Collection

L7: Entry 9 of 19 File: USPT Jun 30, 1998

DOCUMENT-IDENTIFIER: US 5774667 A
TITLE: Method and apparatus for managing parameter settings for multiple network devices

Detailed Description Text (8):
To control the network devices coupled to the Local Area Network 100, the network management workstation 110 executes a network management program 225. The network management program monitors the network segment 100 for network status messages such as SNMP traps. The network management program 225 also polls the various network devices to obtain information from those network devices. The status of the network devices can be displayed graphically on the display screen coupled to the network management workstation 110. To effect changes requested by a user, the network management program 225 sends requests to the manageable network devices.